

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

FILED IN U.S. DISTRICT COURT
DISTRICT OF UTAHfor the
District of Utah

JUN 27 2023

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 INFORMATION ASSOCIATED WITH APPLE ID
 NATIVE_DINE25@YAHOO.COM and
 SHERELDONYANITO@YAHOO.COM

BY GARY P. SEDAR
 CLERK OF COURT
 DEPUTY CLERK
 Case No. 4:23-mj-00100 PK
4:23-mj-00101 PK.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A from Affidavit of TFO Paul Tittensor

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B from Affidavit of TFO Paul Tittensor

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Distribution of fentanyl resulting in death

The application is based on these facts:

See Affidavit of TFO Paul Tittensor

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 6-27-2023

City and state: St. George, Utah

/s/ Paul Tittensor

Applicant's signature

Paul Tittensor, DEA Task Force Officer

Printed name and title

Judge's signature

Paul Kohler, U.S. Magistrate Judge

Printed name and title

TRINA A. HIGGINS, United States Attorney (#7349)
BRADY WILSON, Assistant United States Attorney (#17350)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4266
brady.wilson@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
WARRANT AUTHORIZING THE SEARCH OF
INFORMATION ASSOCIATED WITH APPLE
ID'S (1) NATIVE_DINE25@YAHOO.COM;
and (2) SHERELDONYANITO@YAHOO.COM;
THAT IS STORED AT PREMISES
CONTROLLED BY APPLE, INC.

~~**FILED UNDER SEAL**~~

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A
SEARCH WARRANT

Case No.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, PAUL TITTENSOR, Task Force Officer, Drug Enforcement Administration,
being duly sworn, states:

I. AFFIANT BACKGROUND AND QUALIFICATIONS

1. I am currently a Task Force Officer (TFO) assigned to the United States Drug Enforcement Administration (DEA) Metro Narcotics Task Force (MNTF) in Salt Lake City, Utah. I am an investigative or law enforcement officer of the United States,

within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I am currently assigned to Task Force Group 1 in the DEA Salt Lake City District Office (SLCDO). The SLCDO houses a multi-agency task force responsible for investigating major drug trafficking organizations. In the course of my employment, I have attended numerous schools, trainings and conferences related to drug investigations. In addition to my training, I have participated in numerous drug investigations and, as such, I have experience with the methods used in conducting drug trafficking investigations, including, but not limited to, debriefing cooperating witnesses and confidential sources, conducting controlled purchases of drugs using confidential sources, engaging in undercover negotiations/purchasing drugs in an undercover capacity, surveillance, the preparation of affidavits, the execution of search warrants and court orders and making arrests. Moreover, I have also participated in previous Title III narcotics investigations during which I have analyzed telephone records and have reviewed intercepted conversations. As a result of my training and experience, I am familiar with the methods used by drug traffickers to smuggle, safeguard, store, transport, and distribute controlled substances, and to collect, conceal, and transport the financial proceeds that result from such activities.

2. I have participated in numerous investigations in which drug traffickers relied heavily upon telephones to communicate with their associates, confidential informants, cooperating individuals, and undercover officers. I have also interviewed individuals who have been directly and indirectly involved in the importation,

transportation, and distribution of illegal drugs and controlled substances; and I have worked and consulted with numerous law enforcement officers experienced in drug investigations. As a result, I am familiar with how drug traffickers speak to each other and generally conduct business. For example, I am aware that drug traffickers discussing criminal matters over the phone or electronic messaging often speak vaguely, or in code. This training and experience form the basis for opinions expressed below.

II. PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of an application for search warrants for information associated with two accounts that are stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. I have personally participated in the investigation set forth below. As a result of my personal participation in this investigation, I am familiar with all aspects of this investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that information was provided by another agent, law enforcement officer or

witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the requested information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested search warrant should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this affidavit.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 846, conspiracy to possess with intent to distribute, and conspiracy to distribute, a controlled substance; 21 U.S.C. § 841(a)(1), possession with intent to distribute and distribution of a controlled substance; 21 U.S.C. § 843 (b), unlawful use of a communications facility; and 18 U.S.C. § 1957, engaging in monetary transactions in property derived from specified unlawful activity (the "TARGET OFFENSES"); have been committed by Shereldon YANITO. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, and 18 U.S.C. §§ 2703(a),

(b)(1)(A), and (c)(1)(A). Specifically, the Court is the District Court of the United States District of Utah that has jurisdiction over the offense being investigated.

III. PROBABLE CAUSE

7. As set forth in more detail below, I believe that information held by Apple, Inc. is likely to contain evidence, to assist in obtaining evidence, and be evidence, of the TARGET OFFENSES. The investigation of Shereldon YANITO revealed that he utilized electronic devices to arrange the distribution of controlled substances. Additionally, investigators learned that YANITO likely utilized an Apple iPhone from September 1, 2019 until his arrest on or about May 22, 2023.

8. On or about April 15, 2022, the San Juan County Sheriff's Office and Grand County Sheriff's Office responded to a suspected overdose death of Person 1. The initial officers conducted a crime scene survey, and located several pieces of wrinkled-up aluminum foil in a nearby trash can. The aluminum foil had burns on one side and a burned residue on the other side, which characteristics are consistent with aluminum foil used to ingest a controlled substance. Investigators also located a rolled-up \$5.00 bill was found, which led officers to believe Person 1 had likely ingested a controlled substance by means of inhalation. Witness 1, who had found Person 1 deceased, advised investigators that Person 1 had been inquiring about where he/she could acquire controlled substances in the week prior to Person 1's death.

9. Following a post-mortem examination, Erik D. Christensen, M.D. concluded that Person 1 died as a result of Fentanyl intoxication.

10. Agents interviewed Person 1's associates. Witness 2 advised investigators that Person 1 had been purchasing counterfeit Percocet pills which Person 1 knew to contain Fentanyl. According to Witness 2, Person 1 had been attempting to stop using the counterfeit Percocet pills and had even moved out of the area in an attempt to distance him/herself from the person who provided Person 1 with Fentanyl. Witness 2 advised investigators that Person 1 acquired Fentanyl from Shereldon YANITO (a/k/a "Bobby") and others.

11. During a follow-up interview with Witness 1, Witness 1 advised that he spent time with Person 1 the night before he/she died. According to Witness 1, Person 1 had been struggling with addiction, but was attempting to stop using Fentanyl. Witness 1 informed investigators that he had made a purchase of Fentanyl for himself from "Bobby," who Witness 1 confirmed to be YANITO, using Venmo to make the payment to YANITO. Witness 1 stated that he knew Person 1 got the Fentanyl pill from YANITO, because YANITO sent him a Snapchat message saying he had sold "something" to Person 1. According to Witness 1, YANITO sold counterfeit blue "M30" pills containing Fentanyl to multiple people, including himself, Person 1, and another person who had overdosed and nearly died. Witness 1 stated that when he first began acquiring blue "M30" pills from YANITO, he believed them to be legitimate

pharmaceuticals but only learned later that they contained fentanyl.¹ Witness 1 reported that YANITO charged \$40 per pill for counterfeit "M30" pills containing Fentanyl.

12. Witness 3, a family member of Person 1's, advised that she had seen Person 1 on the night immediately prior to his/her death. According to Witness 3, she observed a Venmo transaction from Person 1 to YANITO'S Venmo account the night before Person 1's death. Agents later confirmed the \$40 Venmo transaction between Person 1 and an account associated with YANITO. Financial research revealed that on April 14, 2022 at 7:38:27 PM, a Venmo account associated with YANITO received a payment of \$40.00 from Person 1 with the comment for item as the "fire emoji".² Investigators also confirmed that on the same date, the same Venmo account associated with YANITO received a payment of \$40 from Witness 1.

13. On or about June 19, 2022, deputies with the Grand County Sheriff's Office and emergency medical personnel responded to a call of an unresponsive person in the 1300 block of Red Valley Court in Moab, Utah. Upon arrival, they observed YANITO on the couch in a confused state. YANITO'S father, who was present at the residence, provided officers with multiple unidentified pills that he had reportedly located in YANITO'S bedroom. Shortly after the Grand County Sheriff's Department left the

¹ Based upon my training and experience, I know that legitimate pharmaceuticals are required by law to bear unique identifying markings. Some forms of legitimate pharmaceutical oxycodone (a Schedule II controlled substance available only by prescription) are marked "M30" and are blue in color.

² Based upon my training and experience, I know that the term "fire" or the "fire emoji" icon are used by individuals using and/or trafficking in controlled substances to signify that a particular controlled substance is very high quality.

residence, YANITO'S mother summoned them back to the residence. She advised that she had located several small blue pills in the garage near where YANITO plays video games. The pills were stamped "M30" and subsequently tested positive for opioids.

14. On or about June 27, 2022, Grand County Sheriff's Deputies had a follow-up conversation with YANITO'S mother regarding the blue "M30" pills. YANITO'S mother was advised that the "M30" pills were Fentanyl pills and were highly dangerous. After YANITO'S mother explained that YANITO was attempting to stop using the blue pills but could not do so, she was advised that it might be prudent for her to obtain some Narcan to have in the house in case of an accidental overdose.³ At that point, YANITO'S mother indicated that she had been carrying Narcan and that she had administered some to YANITO shortly before the ambulance had arrived at their home on June 19, 2022.

15. On or about June 24, 2022, a deputy with the Grand County Sheriff's Office conducted a traffic stop on Witness 4. The traffic stop was wholly unrelated to the death of Person 1. After being advised of his *Miranda* rights, Witness 4 advised that he wished to provide information regarding persons in Grand County who were selling "blues" containing Fentanyl. According to Witness 4, he felt compelled to provide the information because these people were selling "blues" to "little kids." After providing information about two people selling "blues," Witness 4 was asked about "Bobby" YANITO. Witness 4 then stated that "Bobby" had told him that he ("Bobby") had "killed

³ Based upon my training and experience, I know that Narcan is the brand-name for Naloxone, which is a fast-acting opioid antagonist which reverses the effects of opioids. Patients who receive Narcan often wake up feeling confused, disoriented, and sometimes, combative.

a kid.” When asked whether he knew the victim’s name, Witness 4 provided Person 1’s correct first name. Witness 4 explained that shortly after Person 1’s death, Witness 4 and YANITO were hanging out at Witness 4’s place when YANITO told Witness 4 about “killing [Person 1].” Witness 4 described YANITO as “sad about it” and “crying.”

16. On or about May 22, 2023, DEA Task Force Officer Sarah Mullen, acting in an undercover capacity, sent a text message to YANITO’S known cell phone number. Although TFO Mullen and YANITO had no prior relationship, TFO Mullen claimed the two had met before. TFO Mullen advised YANITO that she would be traveling through the Moab area and was interested in purchasing “blues.” After instructing TFO Mullen to contact him via Instagram (a social media application that allows the sharing of photographs and text), YANITO sent TFO Mullen a copy of a photograph she had posed on her undercover Instagram page. The photo depicted a small bag of “blues.” YANITO questioned TFO Mullen about the “blues,” and he stated that he did not have any “blues” and that few people in the area were still using them because so many people had “OD’d” on them. YANITO also commented on how expensive “blues” cost, noting that when he had them, he sold them for \$40 per pill before the price dropped to \$35.

17. Following some additional messages regarding powder cocaine, YANITO agreed to meet TFO Mullen at her hotel room. Surveillance agents observed YANITO at his residence and observed YANITO utilizing a cell phone to communicate with TFO Mullen as messages were being sent back and forth. Agents observed YANITO leave his known residence in a vehicle known to be associated with YANITO. Before he reached the hotel, YANITO was the subject of a traffic stop. At the time of his arrest, a red-

colored Apple iPhone was found in the vehicle. No other electronic device or devices capable of communication were found in the vehicle. YANITO was arrested and transported to the Grand County Jail, where he was advised of his *Miranda* rights. Although he invoked his right to remain silent, YANITO continued to speak despite not being questioned, volunteering that he was not involved in drugs anymore and that he believed he was being targeted because he was the "only one still around" while other involved in the same activity had left town.

18. On May 25, 2023, agents were granted a search warrant to conduct a forensic analysis of the red-colored Apple iPhone, which had been in YANITO'S custody at the time of his arrest. The search warrant was granted by U.S. Magistrate Judge Paul Kohler, and the search warrant was executed on the same date.

19. On June 7, 2023, YANITO was indicted by Grand Jury for 21 U.S.C. 841 (a)(1) Distribution of Fentanyl Resulting in Death.

20. Agents have reviewed the data that was forensically extracted from YANITO'S Apple iPhone, and learned YANITO had been actively backing up data to Apple iCloud as recently as April 9, 2023. Agents observed there were two iCloud accounts utilized by YANITO, iCloud ID native_dine25@yahoo.com and iCloud ID shereldonyanito@yahoo.com. Additionally, information learned through the forensic download indicates that YANITO has previously utilized an Apple iPhone 11 Pro, which was released in September 2019.

21. In the month of June, 2023, agents have identified multiple juvenile witnesses, who have indicated YANITO had been selling cocaine and other drugs to them as recently as a few weeks prior to YANITO'S arrest.

22. Because of, in part, the information contained in paragraph 20, investigators believe that during the timeline of Person 1's death, YANITO was utilizing his Apple electronic devices, and there is a likelihood that information was backed up to the iCloud that could reasonably contain information regarding YANITO'S drug distribution in general but also specifically related to Person 1's overdose death.

23. I know through training and experience that Apple iCloud can retain photographs, communications (including encrypted), GPS location data, in addition to storing data from third-party providers that could benefit this investigation.

IV. BACKGROUND CONCERNING APPLE⁴

24. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac operating system.

⁴ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; "Manage and use your Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "Introduction to iCloud," available at <https://support.apple.com/kb/PH26502>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

25. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers,

Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

26. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users

can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

27. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

28. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes

Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

29. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

30. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected

services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

31. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

32. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

33. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

34. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

35. Other information connected to an Apple ID may lead to the discovery of additional evidence. YANITO has been identified as using CashApp and Venmo financial applications to accept payment for controlled substances he has sold. Agents know through interviews, that YANITO has utilized other applications and encrypted

applications to further his drug trade. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

36. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services – in this case, those of Shereldon YANITO. In my training and experience, such information may constitute evidence of the crimes under investigation, including information that can be used to identify the account user or users.

V. CONCLUSION

37. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the iCloud information associated with the two-captioned Apple IDs used by Shereldon YANITO were used in furtherance/facilitation of illegal drug trafficking, and that the information sought herein will materially aid the investigation.


38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable

cause exists to permit the execution of the requested warrant at any time in the day or night.

RESPECTFULLY SUBMITTED this 26th day of June, 2023.

/s/ Paul Tittensor
PAUL TITTENSOR, Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me this 27 day of June, 2023.



PAUL KOHLER
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with iCloud ID native_dine25@yahoo.com and iCloud ID shereldonyanito@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 26, 2023, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"),

Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and

bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.